Peter H. Burke*
James Harrell
CRUMLEY ROBERTS, LLP
2400 Freeman Mill Road, Suite 200
Greensboro, NC 27406
Telephone: (366) 333-9899
phburke@crumleyroberts.com
jrharrell@crumleyroberts.com

Attorneys for Plaintiff and Proposed Plaintiff's Class Counsel

Karen Hanson Riebel*
Kate M. Baxter-Kauf*
Maureen Kane Berg*
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com
mkberg@locklaw.com

** Special Appearances Entered*

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF NORTH CAROLINA

AFRIKA WILLIAMS, on behalf of herself and all others similarly situated,

Plaintiff,

v.

DUKEHEALTH,
and a Defendant Class of
Facebook Partner Medical Providers,

Defendant.

Case No. 1:22-cv-00727-WO-JEP

AMENDED COMPLAINT – CLASS ACTION

DEMAND FOR JURY TRIAL

Plaintiff Afrika Williams, on behalf of herself and all others similarly situated, allege as follows upon personal knowledge as to her own conduct and on information and belief as to all other matters, based on investigation by counsel, such that each allegation

has evidentiary support or is likely to have evidentiary support upon further investigation and discovery:

I. INTRODUCTION

1. Plaintiff brings this action on behalf of herself and millions of other Americans whose medical privacy has been violated by Facebook's Pixel tracking tool. As explained herein, Defendant knows (or should have known) that Facebook's Pixel tracking tool is being improperly used on its hospital websites, resulting in the wrongful, contemporaneous, re-direction to Facebook of patient communications to register as a patient, sign-in or out of a supposedly "secure" patient portal, request or set appointments, or call their provider via their computing device. This unlawful transmission and collection of data is done without the knowledge or authorization of the patients, like Plaintiff, in violation of Defendant's contracts with its users/patients, as well as in violation of various federal and state laws.

2. When a patient communicates with a health care provider's website where the Facebook Pixel is present on the patient portal login page, the Facebook Pixel source code causes the exact content of the patient's communication with their health care provider to be re-directed to Facebook in a fashion that identifies them as a patient.

3. For example, Plaintiff Williams is a patient of Defendant DukeHealth. In the course of receiving medical care at DukeHealth, Plaintiff Williams has used the "DukeMyChart" patient portal to review her lab results, make appointments, and communicate with her providers.

4. Unbeknownst to Plaintiff, and millions of other patients around the country, when they signed into their patient portals, the Facebook Pixel secretly deployed on the webpage sent to Facebook the fact that they had clicked to sign-in to the patient portal.

5. The data that the Facebook Pixel causes to be re-directed from the patient's computing device to Facebook includes:

a. That the patient was communicating with their healthcare institution via its online patient portal;

b. That the patient engaged in an 'ev' or event called a SubscribedButtonClick;

c. That the content of the button the patient clicked was "Login to" the patient portal;

d. That the page from which the button the patient clicked was Patient Portal – *i.e.* Home;

e. That the patient had previously been at a patient portal page about a particular health area/concern;

f. The patient's Internet Protocol address;

g. Identifiers that Facebook uses to identify the patient and his/her device, including cookies named c-user, datr, fr, and fbp (*i.e.* Facebook Pixel); and

h. Browser attribute information sufficient to fingerprint the patient's device.

6. As explained in further detail below, patient-status is protected by HIPAA, which requires a valid HIPAA-compliant authorization before it is conveyed by medical providers or collected by Facebook.

7. Neither Facebook nor the Defendant or members of the Defendant class of health care institutions that deployed the Facebook Pixel on their web properties ("Facebook Partner Medical Providers") procured HIPAA authorizations for the disclosure of patient status and health information to Facebook.

8. In the absence of a HIPAA authorization, Facebook's collection of patient status and the content of patient communications with the Facebook Partner Medical Providers, including when patients register, log-in and logout of patient portals and set up appointments, violates Defendant's privacy promises to users.

9. Facebook promises users that "publishers can send us information through Meta Business Tools [such as] the Meta Pixel" but Facebook "require[s] each of these partners to have lawful rights to collect, use, and share your data before providing any data to us."

10. The Facebook Partner Medical Providers promise their patients/website users that they will protect the privacy of the patients' health information; that they will use and disclose their health information only for enumerated, permitted purposes, and that they will obtain the patient's/user's consent before disclosing their health information for any non-enumerated purpose (Facebook Partner Medical Providers' Privacy Notices).[1] The Facebook Partner Medical Providers' Privacy Notices are substantively identical or very similar on these points, as they are largely dictated by law, including HIPAA.

[1] *See, e.g.*, DukeHealth's Notice of Privacy Practices, located at: https://www.dukehealth.org/sites/default/files/notice-privacy-brochure.pdf (last accessed July 24, 2023).

11. However, Facebook knowingly receives, and the Facebook Partner Medical Providers knowingly convey, patient data—including patient portal usage information—from hundreds of Facebook Partner Medical Providers in the United States that have deployed the Facebook Pixel on their web properties, including Defendant.

12. On information and belief, at least 664 hospital systems or medical provider web properties convey patient data to Facebook via the Facebook Pixel.

13. Despite knowingly receiving health-related information from Facebook Partner Medical Providers, Facebook has not taken any action to enforce or validate its requirement that Facebook Partner Medical Providers obtain adequate consent from patients before providing patient data to Facebook.

14. Despite knowingly conveying health-related information to Facebook via the Facebook Pixel, the Facebook Partner Medical Providers have not obtained adequate consent from patients before providing patient data to Facebook.

15. Facebook monetizes the information it receives through the Facebook Pixel deployed on medical providers' web properties by using it to generate highly-profitable targeted advertising on- and off-Facebook.

16. The targeted advertising Facebook offers for sale includes the ability to target patients based on specific actions that a patient has taken on the Facebook Partner Medical Providers' websites.

17. Facebook also offers the ability to engage in remarketing based on positive targeting – that is, serving specific ad campaigns to patients based on the specific actions those patients took on the Facebook Partner Medical Providers' websites. For example,

Facebook could target ads to a patient who had (1) used the patient portal and (2) viewed a page about a specific condition, such as cancer.

18. Facebook also offers Facebook Partner Medical Providers the ability to engage in remarketing based on negative targeting – that is, ensuring that ads are not shown to users who have taken specific action. This could mean that Facebook would exclude existing patients from a Facebook Partner Medical Provider's advertising campaign in order to establish new patients.

19. Facebook employs thousands of account managers or representatives to help partners, including Facebook Partner Medical Providers, use the Facebook Pixel and other tools.

20. Through its account managers and representatives, Facebook is aware that it is receiving patient data from hundreds of different Facebook Partner Medical Providers in the United States without patient knowledge, consent, or valid HIPAA authorizations.

21. Facebook also utilizes "The Facebook Crawler" that scans pages of partner apps and websites and through which Facebook gathers information about the app or website, including its title and description.

22. Through the Facebook Crawler, Facebook is aware that it is receiving patient data.

23. Facebook has also been served subpoenas in other actions regarding disclosure of patient information through the Facebook Pixel, and litigation regarding this issue has been severed from this case and transferred to the United States District Court for the Northern District of California. *See In re Meta Pixel Healthcare Litigation*, No. CV

22-03580-WHO (N.D. Cal.) (Orrick, J.) (containing claims against Facebook originally filed in the instant action and transferred).

24. Facebook is also aware of every web property where the Facebook Pixel is deployed and Facebook is fully capable of conducting expert analysis to identify hospitals or medical provider properties where the Facebook Pixel is present.

25. Facebook Partner Medical Providers are aware through their web developers and other IT professionals, and additional employees, that the Facebook Pixel is conveying protected patient data to Facebook.

26. Facebook Partner Medical Providers' actions give rise to causes of action for (1) breach of contract; (2) intrusion upon seclusion/breach of privacy; (3) federal electronic communications privacy and wiretap claims; (4) negligent misrepresentation; and (5) negligence; including negligence *per se*.

II. JURISDICTION AND VENUE

27. This Court has personal jurisdiction over the Defendant because DukeHealth has sufficient minimum contacts with this District and operates and markets its services throughout the state and in this District. Additionally, Defendant DukeHealth is headquartered in this District.

28. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because this action arises under 18 U.S.C. § 2510, *et seq.*, (the Electronic Communications Privacy Act). This Court further has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d) (the Class Action Fairness Act) because the amount in controversy exceeds

$5,000,000, exclusive of interest and costs, and a member of the Class is a citizen of a State different from any Defendant.

29. This Court has supplemental jurisdiction over the remaining state law claims pursuant to 28 U.S.C. § 1367 because the state law claims form part of the same case or controversy under Article III of the United States Constitution.

30. Venue is proper in this district because Defendant DukeHealth is headquartered in this District and resides this this District, and substantial parts of the events or omissions giving rise to the claims occurred in or emanated from this District.

III. PARTIES TO THE LITIGATION

31. Plaintiff Afrika Williams is a citizen of North Carolina, residing in Morrisville, North Carolina, a Facebook user, and a patient of Defendant DukeHealth ("DukeHealth"), who used the "DukeMyChart" patient portal, currently located at https://www.dukemychart.org/home/Authentication/Login?%5Fga=2%2E45171425%2E430573737%2E1660242258%2D451756755%2E1660242258, to view medical records, lab results, and otherwise communicate with her provider. Plaintiff's use of DukeHealth's patient portals included the time during which the Facebook Pixel was secretly deployed on the portal login pages.

32. Defendant DukeHealth is a not-for-profit health system organized under the laws of North Carolina and headquartered in Durham, North Carolina. Its DukeMyChart patient portal uses the Facebook Pixel, through which it conveyed Williams's patient status and health information to Facebook.

IV. FACTS COMMON TO ALL COUNTS

A. HEALTH PRIVACY LAWS IN THE UNITED STATES

33. Patient health care information in the United States is protected by federal law under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations promulgated by the United States Department of Health and Human Services ("HHS").

34. The HIPAA Privacy Rule establishes "national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as "protected health information" or "PHI") and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization. The Rule also gives individuals rights over their protected health information, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their protected health information in an electronic health record, and to request corrections. The Privacy Rule is located at 45 CFR Part 160 and Subparts A and E of Part 164." https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

35. Under 45 C.F.R. § 164.502, a health care provider or business associate of a health care provider "may not use or disclose 'protected health information' except as permitted or required by" the HIPAA Privacy Rule.

36. Under 45 C.F.R. 160.103, the Privacy Rule defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

37. Under 45 C.F.R. § 160.103, the Privacy Rule defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

38. Under 45 C.F.R. § 164.514, the HIPAA de-identification rule states that "health information is not individually identifiable only if" (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination,'" or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed: Names ... Medical record numbers; ... Account numbers ... Device identifiers and serial numbers; ... Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; ... and any other unique identifying number, characteristic, or code." In addition, the covered

entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."

39. Under 42 U.S.C. § 1320d-6, any "person [individual ... or a corporation] who knowingly and in violation of this part—(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual ... shall be punished" by fine or, in certain circumstances, imprisonment, with increased penalties for "intent to sell, transfer, or use individually identifiable health information for commercial advantage[.]" The statute further provides that a "person ... shall be considered to have obtained or disclosed individually identifiable health information ... if the information is maintained by a covered entity ... and the individual obtained or disclosed such information without authorization."

40. Patient status alone is protected by HIPAA.

41. Guidance from HHS instructs health care providers that patient status is protected by HIPAA. In Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, HHS sets out:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data. ... *If such information was listed with* health condition, *health care provision* or payment data,

> *such as an indication that the individual was treated at a certain clinic*, then this information would be PHI.[2]

42. In its guidance for Marketing, HHS further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. ... Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*.[3]

43. HHS has previously instructed that HIPAA covers patient-status, i.e., the question whether an individual is a patient of a medical institution:

a. "The sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);

b. "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which would include disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002);

---

2 https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf at 5 (emphasis added).

3 https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/market ing.pdf at 1-2 (emphasis added).

c. It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 Fed. Reg. 5642 (Jan. 25, 2013); and

d. The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1). Even then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R. § 164.510(2).

44. There is no HIPAA-exception for the Internet or online patient portals.

B. FACEBOOK'S CONTRACTUAL PROMISES

45. Every Facebook user is legally deemed to have agreed to the Terms, Data Policy, and Cookie Policy via a checkbox on the sign-up page; and the Terms, Data Policy, and Cookie Policy are binding upon Facebook and its users.

46. The Facebook Data Policy expressly provides that Facebook "requires" businesses that use the Facebook Pixel "to have lawful rights to collect, use, and share your data before providing any data to [Facebook]."

47. But Facebook does not "require" medical providers to have lawful rights to share patient data associated with their respective patient portals and appointment software before sending it to Facebook.

48. Instead, Facebook merely includes a provision in its form contract which creates an unenforced "honor system" for publishers, stating that, by using the Facebook Business Tools, the publisher "represent[s] and warrant[s] that [it has] provided robust and sufficient prominent notice to users regarding the Business Tool Data collection, sharing, and usage."

49. In reality, Facebook does not actually verify that publishers have obtained adequate consent per the contract.[4]

50. Instead, the Facebook Pixel is blindly made available to any willing publisher regardless of their privacy policies, consent processes, or the nature of their business.

51. Facebook's contract with medical providers for use of the Facebook Pixel does not mention HIPAA at all.

52. Facebook actively encourages medical providers to use the Facebook Pixel for their marketing campaigns.

C. HOW THE FACEBOOK PIXEL WORKS

53. Facebook operates the world's largest social media company.

54. Facebook maintains profiles on users that include users' real names, locations, email addresses, friends, likes, and communications that Facebook associates with personal identifiers including IP addresses, cookies, and device identifiers.

55. Facebook also tracks non-users across the web through its widespread Internet marketing products and source code.

[4] In contrast, Facebook requires publishers in the European Union to provide "all necessary consents" in a "verifiable manner."

56. Facebook's revenue is derived almost entirely from selling targeted advertising to Facebook users on Facebook.com and to all Internet users on non-Facebook sites that integrate Facebook marketing source code on their websites.

57. Facebook Business is the division that provides advertising services to developers. Facebook Business and the advertising tools it provides to developers are focused on trade and commerce.

58. The Facebook Pixel, a product for Facebook Business, is a "piece of code" that lets developers "measure, optimize and build audiences for ... ad campaigns."[5]

59. The Facebook Pixel is an invisible 1x1 web bug that Facebook makes available to web-developers to help track ad-driven activity from Facebook and others on their website.

60. Key features of the Facebook Pixel include its ability to help developers:

a. "Measure cross-device conversions" and "understand how your cross-device ads help influence conversion";

b. "Optimize delivery to people likely to take action" and "ensure your ads are shown to the people most likely to take action"; and

c. "Create custom audience from website visitors" and create "dynamic ads [to] help you automatically show website visitors the products they viewed on your website – or related ones."

[5] https://www.facebook.com/business/learn/facebook-ads-pixel

61. Facebook describes the Facebook Pixel as "a snippet of Javascript code" that "relies on Facebook cookies, which enable [Facebook] to match ... website visitors to their respective Facebook User accounts."

62. Facebook further explains "How the Facebook Pixel Works":[6]

> When someone visits your website and takes an action (for example, buying something), the Facebook pixel is triggered and reports this action. This way, you'll know when a customer took an action after seeing your Facebook ad. You'll also be able to reach this customer again by using a custom audience. When more and more conversions happen on your website, Facebook gets better at delivering your ads to people who are more likely to take certain actions. This is called conversion optimization.
>
> *Id.*

63. Facebook provides simple instructions for developers about "Setting up the Facebook Pixel":

> If you have access to your website's code, you can add the Facebook pixel yourself. Simply place the Facebook pixel base code (what you see when you create your pixel) on all pages of your website. Then add standard events to the pixel code on all special pages of your website, such as your add-to-cart page or your purchase page. For full step-by-step instructions or adding the Facebook pixel to your site, visit the Help Center.
>
> Many people need the help of a developer to complete this step. If that's the case, simply email your Facebook pixel code to them, and they can easily add it to your site.
>
> Create your Facebook pixel to send to your developer, or install it yourself.
>
> Go to Ads Manager

[6] https://www.facebook.com/business/learn/facebook-ads-pixel

64. Facebook creates the Facebook code for each developer who installs it.

65. Facebook recommends that the Pixel code be placed early in the source code for any given webpage or website to ensure that the user will be tracked:

> Installing The Pixel
>
> To install the pixel, we highly recommend that you add its base code between the opening and closing <head> tags on every page where you will be tracking website visitor actions. Most developers add it to their website's persistent header, so it can be used on all pages.
>
> Placing the code within your <head> tags reduces the chances of browsers or third-party code blocking the pixel's execution. It also executes the code sooner, increasing the chance that your visitors are tracked before they leave your page.

66. By executing the code sooner, Facebook has designed the Pixel such that Facebook receives the information about patient actions on the medical provider's properties contemporaneous with their making.

67. As soon as a patient takes any action on a webpage which includes the Facebook Pixel—such as clicking a button to register, login, or logout of a patient portal or to create an appointment—Facebook's source code commands the patient's computing device to re-direct the content of the patient's communication to Facebook while the exchange of the communication between the patient and the medical provider is still occurring.

68. By design, Facebook receives the content of a patient's patient portal sign-in communication immediately *after* the patient clicks the log-in button and *before* the medical provider receives it.

69. In all cases, the content of the patient's portal and appointment communications are re-directed to Facebook while the communications are still occurring.

70. The cookies by which Facebook identifies patients include, but are not necessarily limited to, cookies named: c_user, datr, fr, and _fbp.

71. The c_user cookie is a means of identification for Facebook users. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user account has one – and only one – unique c_user cookie. Facebook uses the c_user cookie to record user activities and communications.

72. A skilled computer user can obtain the c_user cookie value for any Facebook user by (1) going to the user's Facebook page, (2) right-clicking on their mouse, (3) selecting 'View page source,' (4) executing a control-F function for "fb://profile," and (5) copying the number value that appears after "fb://profile" in the page source code of the target Facebook user's page.

73. It is even easier to find the Facebook account associated with a c_user cookie: one simply needs to log-in to Facebook, and then type www.facebook.com/#, with # representing the c_user cookie identifier. For example, the c_user cookie value for Mark Zuckerberg is 4. Logging in to Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck.

74. The Facebook datr cookie identifies the patient's specific web browser from which the patient is sending the communication. It is an identifier that is unique to the patient's specific web browser and is therefore a means of identification for Facebook users.

75. Facebook keeps a record of every datr cookie identifier associated with each of its users, and a Facebook user can obtain a redacted list of all datr cookies associated with his or her Facebook account from Facebook.

76. Any Facebook user can view the specific datr cookie identifiers that Facebook has associated with their account by using the Facebook Download Your Information tool.

77. The Facebook fr cookie is an encrypted combination of the c_user and datr cookies.[7]

78. The Facebook _fbp cookie is a Facebook identifier that is set by Facebook source code and associated with Defendant's use of the Facebook Pixel. The _fbp cookie is a Facebook cookie that masquerades as a first-party cookie to evade third party cookie blockers and share data more directly between a medical provider and Facebook.

79. The medical provider or its developer then simply copy-pastes the Facebook Pixel code that Facebook creates and provides into the medical provider's web-property.

80. Facebook expressly admits that the Pixel "log[s] when someone takes an action" such as "adding an item to their shopping cart or making a purchase."

> Once you've set up the Meta Pixel, the Pixel will log when someone takes an action on your website. Examples of actions include adding an item to their shopping cart or making a purchase. The Meta Pixel receives these actions, or events, which you can view on your Meta Pixel page in Events Manager. From there, you'll be able to see the actions that your

[7] *See* Facebook Tracking Through Social Plug-ins: Technical Report prepared for the Belgian Privacy Commission, Mar. 27, 2015, available at https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf.

customers take. You'll also have options to reach those customers again through future Facebook ads.

81. For medical providers, the actions that the Facebook Pixel logs include:

a. When a patient clicks to register for the patient portal;

b. When a patient clicks to log-in to the patient portal;

c. When a patient clicks to logout of the patient portal;

d. When a patient sets up an appointment;

e. When a patient clicks a button to call the provider; and

f. The specific communications a patient exchanges at the provider's property, including those relating to specific providers, conditions, and treatments and the timing of such actions, including whether they are made while a patient is still logged-in to a patient portal or around the same time that the patient has scheduled an appointment, called the medical provider, or logged in or out of the patient portal.

D. FACEBOOK PUBLICLY ACKNOWLEDGES THAT HEALTH-BASED ADVERTISING IS INAPPROPRIATE

82. Facebook has publicly acknowledged that targeted advertising based on health information is not appropriate.

83. On November 9, 2021, Facebook announced that it was removing the ability to target users on "topics people may perceive as sensitive, such as options referencing causes, organizations, or public figures that relate to health[.]"[8]

84. Facebook's announcement was a public relations success:

a. Reuters published a story headlined "Facebook plans to remove thousands of sensitive ad-targeting options" and led the story with a sentence about Facebook's "plans to remove detailed ad-targeting options that refer to 'sensitive' topics, such as ads based on interactions with content around ... health[.]"[9]

b. The New York Times published a similar story with a similar headline, "Meta plans to remove thousands of sensitive ad-targeting categories: Ad buyers will no long be able to use topics such as health ... to target people[.]"[10]

c. Many more, similar, articles were published, giving Facebook's users the misimpression that Facebook would not allow targeting based on health.

85. But Facebook did not change the most insidious types of targeting based on health: those marketing campaigns from medical providers that disclose patient identities

[8] https://www.facebook.com/business/news/removing-certain-ad-targeting-options-and-expanding-our-ad-controls

[9] https://www.reuters.com/technology/facebook-removes-target-options-advertisers-some-topics-2021-11-09/

[10] https://www.nytimes.com/2021/11/09/technology/meta-facebook-ad-targeting.html

and their individually identifiable health information to Facebook for the purpose of targeted marketing based on their communications with their medical providers.

86. Facebook clarified that the change was limited to "people's interactions with content" on the Facebook "platform."

87. Facebook then informed advertisers that they could still use "website custom audiences and lookalike" to "help reach people who have already engaged with a business or group's website or products." In the case of medical providers, the "people who have already engaged" are patients.

E. FACEBOOK CHANGED ITS CONTRACTUAL PRIVACY PROMISES IN 2018

88. Prior to April 2018, Facebook's contract did not "require" partners to have the lawful rights to share user data before doing so.

89. Upon information and belief, Facebook changed its contract with users on or about April 19, 2018, which added a clause stating: "We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us."

90. The following is a side-by-side comparison of the pre- and post-April 2018 contract provisions:

Before April 19, 2018	After April 19, 2018
Information from websites and apps that use our Services. We collect information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button or Facebook Log In or use our measurement and advertising services). This includes information about the	**Information from partners.** Advertisers, app developers, and publishers can send us information through Meta Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Meta pixel. These partners provide information about your activities

websites and apps you visit, your use of our Services on those websites and apps, as well as information the developer or publisher of the app or website provides to you or us. **Information from third-party partners.** We receive information about you and your activities on and off Facebook from third-party partners, such as information from a partner when we jointly offer services or from an advertiser about your experiences or interactions with them.	off of our Products—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services—whether or not you have an account or are logged into our Products. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information. Partners receive your data when you visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us. Learn more about the types of partners we receive data from. To learn more about how we use cookies in connection with Meta Business Tools, review the Facebook Cookies Policy and Instagram Cookies Policy.

F. FACEBOOK PARTNER MEDICAL PROVIDERS' CONTRACTUAL PROMISES

91. The Facebook Partner Medical Providers, including Defendant, make substantively identical or extremely similar promises in their Privacy Notices, including promises that they will protect the privacy of their patients' health information; that they will use and disclose their health information only for enumerated, permitted purposes, and that they will obtain the patient's consent before disclosing their health information for any non-enumerated purpose.

V. CLASS ACTION ALLEGATIONS

A. PLAINTIFF CLASS ALLEGATIONS

92. Plaintiff files this as a class action on behalf of herself and the following class pursuant to Fed. R. Civ. P. 23(a) and 23(b)(3):

> All Facebook users who are current or former patients of medical providers in the United States with web properties through which Facebook acquired patient communications relating to medical provider patient portals, appointments, phone calls, and communications associated with patient portal users, for which neither the medical provider nor Facebook obtained a HIPAA, or any other valid, consent.

93. Where appropriate, the above-defined class is referred to as the "Plaintiff Class."

94. Excluded from the Plaintiff Class are the Court and its personnel and the Defendant and its officers, directors, employees, affiliates, legal representatives, predecessors, successors and assigns, and any entity in which any of them have a controlling interest.

95. Plaintiff reserves the right to amend the class definitions, including creating subclasses as necessary, after having had an opportunity to conduct discovery.

96. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

97. **Numerosity.** Consistent with Fed. R. Civ. P. 23(a)(1), the members of the Plaintiff Class are so numerous that joinder is impracticable. While the exact number of

Class Members is unknown to Plaintiff at this time, the proposed Class includes at least tens of thousands of individuals who may be identified through objective means.

98. **Commonality and Predominance.** Consistent with Fed. R. Civ. P. 23(a)(2) and 23(b)(3), common questions of law and fact are apt to drive resolution of the case, exist as to all members of the Plaintiff Class and predominate over any questions affecting solely individual members of the Plaintiff Class including, but not limited to, the following:

a. Whether the Facebook Pixel is designed to send individually identifiable information to Facebook;

b. Whether the Defendant's Terms and Privacy Notices are valid contracts;

c. Whether Facebook failed to require Facebook Partner Medical Providers to have lawful rights to share patient data with Facebook before deploying the Facebook Pixel;

d. Whether Facebook acquired the content of patient communications;

e. Whether the Plaintiff Class provided Defendant with authorization for Facebook to acquire their communications with their medical providers, including through the patient portal, appointment forms, and phone calls;

f. Whether the Facebook Pixel's presence and use on Facebook Partner Medical Provider websites where it discloses actions that patients take relating to patient portals, appointments, and phone calls to their Facebook Partner Medical Providers is highly offensive;

g. Whether Facebook's acquisition of the content of communications between patients and their Facebook Partner Medical Providers occurred contemporaneously to their making;

h. Whether Defendant breached its contracts with users;

i. Whether the information at issue has economic value; and

j. Whether Defendant unjustly profited from its conveyance and collection of patient portal, appointment, and phone call information.

99. **Typicality.** Consistent with Fed. R. Civ. P. 23(a)(3), the named Plaintiff's claims are typical of the claims of other Plaintiff Class Members, as all members of the Class were similarly affected by Defendant's wrongful conduct in violation of federal and state law, as complained of herein.

100. **Adequacy.** Consistent with Fed. R. Civ. P. 23(a)(4), the named Plaintiff will fairly and adequately protect the interests of the members of the Plaintiff Class and has retained counsel that is competent and experienced in class action litigation. The named Plaintiff has no interests that conflict with, or are otherwise antagonistic to, the interests of, other Plaintiff Class Members.

101. **Superiority.** Consistent with Fed. R. Civ. P. 23(b)(3), a class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all Plaintiff Class Members is impracticable. Further, as the damages that individual Plaintiff Class Members have suffered may be relatively small, the expense and burden of individual litigation make it impossible for members of the Plaintiff

Class to individually redress the wrongs done to them. There will be no difficulty in management of this action as a class action.

102. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the common questions of law and fact predominate over any questions affecting individual Class Members, a class action is superior to other available methods for the fair and efficient adjudication of this controversy, and the requirements of Rule 23(a) are met.

B. DEFENDANT CLASS ALLEGATIONS

103. Plaintiff also brings this action as a defendant class action pursuant to Federal Rules of Civil Procedure 23(a) and (b)(1)(A) and (B) against a class consisting of Defendant health care institutions that deployed the Facebook Pixel on their web properties, including Defendant and the Facebook Partner Medical Providers (the "Defendant Medical Providers Class" or "Defendant Class").

104. Excluded from the Defendant Medical Provider Class is WakeMed, who was previously named as a defendant in this action and for whom claims are proceeding in North Carolina State Court.

105. The members of the Defendant Medical Provider Class are so numerous that joinder of all members is impracticable. Upon information and belief, there are approximately 664 members of the Defendant Class.

106. There are questions of law and fact that are common to the Defendant Class. These questions include, but are not limited to:

(1) whether their Privacy Notices constitute contracts with their patients/users;

(2) whether their use of the Facebook Pixel and resulting conveyance of patient status and health information to Facebook violated those contracts;

(3) whether their conveyance of patient status and health information to Facebook constitutes an invasion of privacy/intrusion upon seclusion;

(4) whether their conveyance of patient status and health information to Facebook damaged Plaintiff and the members of the Plaintiff Class;

(5) whether their conveyance of patient status and health information to Facebook and resultant damage to their patients constitutes negligence;

(6) whether their conveyance of patient status and health information to Facebook violates HIPAA, the ECPA, or other federal or state statutes;

(7) whether such violations of HIPAA, the ECPA, or other federal or state statutes constitutes negligence *per se*;

(8) whether their conveyance of patient status and health information to Facebook constitutes a privacy violation that supports Article III standing.

107. The named individual medical provider Defendant above should be appointed, without cost to the class, as representative of the Defendant Medical Provider Class (the "Defendant Class Representative").

108. The claims against and anticipated defenses of the Defendant Class Representative are typical of the claims against and anticipated defenses of the unnamed members of the Defendant Class. Like the Defendant Class Representative, each of the unnamed members of the Defendant Class voluntarily deployed the Facebook Pixel on their web properties resulting in the wrongful, contemporaneous, re-direction to Facebook

of patient communications to register as a patient, sign-in or out of a supposedly "secure" patient portal, request or set appointments, or call their provider via their computing device. The nature of the defenses that may be asserted by the Defendant Class Representative also would be the same, as liability for disclosure of patient status and health information does not depend on the personal circumstances of the particular Defendant Class Members.

109. The Defendant Class Representative will be an adequate and appropriate representative of the Defendant Class in the course of and by virtue of its own defenses to the same claims. Because it has as strong an incentive to vigorously defend against the Plaintiff Class's claims as any unnamed Defendant Class Member, the Defendant Class Representative will fairly and adequately protect and represent the interests of the unnamed members of the Defendant Class.

110. Prosecuting separate actions against individual Defendant Class Members would create a risk of inconsistent judgments with respect to individual class members. If multiple actions against Facebook Partner Medical Providers resulted in, for example, different determinations to the common questions enumerated above, among others, then that would establish incompatible standards for Plaintiff in seeking relief from Defendant Meta and the Defendant Medical Provider Class.

111. Further, as a practical matter, the cost and difficulty of defending against separate suits following the adjudication of the common questions of fact and law related to the Facebook Partner Medical Provider Class's use of the Facebook Pixel on their web properties would be dispositive of or substantially impair the interests of the unnamed Defendant Class Members.

VI. TOLLING

112. Any applicable statute of limitations has been tolled by Defendant's knowing and active concealment of the misrepresentations and omissions alleged herein. Through no fault or lack of diligence, Plaintiff and members of the Plaintiff Class were deceived and could not reasonably discover Defendant's deception and unlawful conduct.

113. Plaintiff and members of the Plaintiff Class did not discover and did not know of any facts that would have caused a reasonable person to suspect that Defendant was acting unlawfully and in the manner alleged herein. As alleged herein, the representations made by Defendant and the Defendant Class were material to Plaintiff and members of the Plaintiff Class at all relevant times. Within the time period of any applicable statutes of limitations, Plaintiff and members of the Plaintiff Class could not have discovered through the exercise of reasonable diligence the alleged wrongful conduct.

114. At all times, Defendant and the Defendant Class are and were under a continuous duty to disclose to Plaintiff and members of the Plaintiff Class the true nature of the disclosures being made and the lack of an actual "requirement" before the data was shared with Facebook.

115. Defendant knowingly, actively, affirmatively and/or negligently concealed the facts alleged herein. Plaintiff and members of the Plaintiff Class reasonably relied on Defendant's concealment.

116. For these reasons, all applicable statutes of limitation have been tolled based on the discovery rule and Defendant's concealment, and Defendant is estopped from relying on any statutes of limitations in defense of this action.

FIRST CAUSE OF ACTION
BREACH OF CONTRACT
(Against Defendant and the Defendant Medical Providers Class)

117. Plaintiff hereby incorporates all prior paragraphs as if fully stated herein.

118. Facebook requires users to click a box indicating that, "By clicking Sign Up, you agree to our Terms, Data Policy and Cookies Policy."

119. "Click-wrap agreements" such as those at issue herein are valid and binding contracts.

120. The Facebook Terms are binding on Facebook and its users.

121. The Facebook Data Policy is binding on Facebook and its users.

122. The Facebook Cookies Policy is binding on Facebook and its users.

123. The Facebook Data Policy promises users that Facebook "requires each of [Facebook's] partners to have lawful rights to collect, use and share your data before providing any data to [Facebook]."

124. The Defendant Medical Providers promise in their Privacy Policies that they will protect the privacy of their patients' health information; that they will use and disclose their health information only for enumerated, permitted purposes, and that they will obtain the patient's consent before disclosing their health information for any non-enumerated purpose.

125. The Defendant Medical Providers breached these contractual promises when they conveyed patient status and health information to Facebook via the Facebook Pixel without obtaining their patients' consent.

126. In addition to the express contract provisions set forth above, implied contracts existed between Defendant and Plaintiff that Defendant would not conspire with others to violate Plaintiff's legal rights to privacy in their individually identifiable health information.

127. Plaintiff the Plaintiff Class are Facebook account holders who used Defendant Medical Providers' patient portals and/or appointment-related functionality of their medical providers' respective web-properties through which Facebook obtained their individually identifiable health information.

128. Plaintiff used the Defendant's patient portal by signing in and out of the portal to access medical records, lab results, and otherwise to communicate with her providers.

129. The patient health information that Defendant Medical Providers conveyed and that Facebook obtained in breach of their contracts with Plaintiff included:

a. Patient identifiers including, but not limited to, email addresses, IP addresses, persistent cookie identifiers, device identifiers, and browser fingerprint information;

b. the data and time of patient registrations for their Defendant Medical Providers' patient portals;

c. log-in and logout times for their Defendant Medical Providers' patient portals;

d. the contents of communications that patients exchange inside their Defendant Medical Providers' patient portals immediately before logging out of those portals;

e. the contents of communications relating to appointments that patients made with their Defendant Medical Providers; and

f. the user's status as a patient of their Defendant Medical Providers.

130. Defendant's breaches caused Plaintiff and Plaintiff Class Members the following damages:

a. Nominal damages for breach of contract;

b. General damages for invasion of their privacy rights in an amount to be determined by a jury without reference to specific pecuniary harm;

c. Sensitive and confidential information including patient status and appointments that Plaintiff and Plaintiff Class Members intended to remain private are no longer private;

d. Defendant eroded the essential confidential nature of the patient-provider relationship;

e. Defendant took something of value from Plaintiff and Plaintiff Class Members and derived benefits therefrom without Plaintiff's and Plaintiff Class Members' knowledge or informed consent and without sharing the benefit of such value;

f. Benefit of the bargain damages in that Defendant's contracts stated that payment for their services would consist of a more limited set of

collection of personal information than that which Defendant actually charged.

SECOND CAUSE OF ACTION
INTRUSION UPON SECLUSION—INVASION OF PRIVACY
(Against All Defendant and the Defendant Medical Providers' Class)

131. Plaintiff hereby incorporates all other paragraphs as if fully stated herein.

132. Plaintiff had no knowledge and did not consent or authorize Defendant Medical Providers to convey or to obtain the content of their communications with her medical providers as described herein.

133. Plaintiff and the Plaintiff Class enjoyed objectively reasonable expectations of privacy surrounding communications with Defendant and Defendant Medical Providers relating to the respective patient portals and appointments based on:

a. The Defendant Medical Providers' status as their health care providers and the reasonable expectations of privacy that attach to such relationships;

b. HIPAA;

c. the Electronic Communications Privacy Act; and

d. Facebook's promise that it would "require" partners to have lawful permission to share their data before Facebook would collect it; and

e. The Defendant Medical Providers' promises to keep their patient status and health information private.

134. Plaintiff's claims are based on the following private facts:

a. that Plaintiff is a patient of the Defendant, a medical provider;

b. The specific dates and times Plaintiff clicked to log-in or log-out of the various medical providers' patient portals;

c. The specific and detailed communications exchanged while logged-in to a patient portal; and

d. The specific dates and times where Plaintiff requested appointments and from which doctor's or practice group pages such appointments were requested.

135. Defendant's conduct was intentional and intruded on Plaintiff's and Plaintiff Class Members' medical communications which constitute private conversations, matters, and data.

136. Plaintiff and the Plaintiff Class suffered a harm from Defendant and the Defendant Class's conduct in conveying private medical information, patient portal, and appointment communications to a third party, Facebook, without permission, and intruded into Plaintiff's peace and quiet in a realm that is private and personal. Defendant, without authorization, invaded Plaintiff's online portal and MyChart, which contained private information, beyond the scope of that which was authorized by Plaintiff and also for the purpose of sharing that information with a third party, Facebook, to use that private matter for marketing. Defendant also allowed Facebook to intrude into Plaintiff's seclusion and online portal without permission by planting a Pixel into the portal and Plaintiff's private information and locations. This is an example of a harm traditionally recognized as a basis for a lawsuit in American courts, and Plaintiff and the Plaintiff class suffered an invasion

of a legally protected interest in privacy. Defendant promised to keep Plaintiff's patient status and health information private, and did not.

137. It is also instructive to read the Court's comments in the case where Plaintiffs' severed claims against Facebook are proceeding: "I think. . . a reasonable Facebook user would be shocked to realize that, if what the plaintiffs are saying is true, [where the pixel is, . . . their health information is going to be sent to Facebook.]" *In re Meta Pixel Healthcare Litigation*, No. CV 22-03580-WHO (N.D. Cal.), 11/9/2022 Transcript at 19-20. Doc. 141.

138. The Defendant Class's conduct in conveying patient portal and appointment communications would be highly offensive to a reasonable person because:

a. Defendant conspired to violate a cardinal rule of the provider-patient relationship;

b. Defendant's conduct violated federal law designed to protect patient privacy;

c. Defendant's conduct violated the ECPA; and

d. Defendant's conduct violated the express promises made to users.

139. Defendant's breaches caused Plaintiff and Plaintiff Class Members the following damages:

a. Nominal damages for breach of contract;

b. General damages for invasion of their privacy rights in an amount to be determined by a jury without reference to specific pecuniary harm;

c. Sensitive and confidential information including patient status and appointments that Plaintiff and Plaintiff Class Members intended to remain private are no longer private;

d. Defendant eroded the essential confidential nature of the patient-provider relationship;

e. Defendant took something of value from Plaintiff and Plaintiff Class Members and derived benefits therefrom without Plaintiff's and Plaintiff Class Members' knowledge or informed consent and without sharing the benefit of such value; and

f. Benefit of the bargain damages in that Defendant's contracts stated that payment for their services would consist of a more limited set of collection of personal information than that which Facebook actually charged.

THIRD CAUSE OF ACTION
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
(Against Defendant and Defendant Medical Providers Class)

140. Plaintiff hereby incorporates all other paragraphs as if fully stated herein.

141. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the contents of any electronic communication. 18 U.S.C. § 2511.

142. The ECPA protects both the sending and receipt of communications.

143. 18 U.S.C. § 2520(a) provides a private right of action to any person whose electronic communications are intercepted.

144. Facebook intentionally intercepted, and Defendant Medical Providers sent to Facebook, the electronic communications that Plaintiff exchanged with their respective Defendant Medical Providers on the providers' web properties where the Facebook Pixel was present.

145. The transmissions of data between Plaintiff and their medical providers qualify as communications under the ECPA's definition in 18 U.S.C. § 2510(12).

146. The Defendant Medical Providers sent, and Facebook acquired, Plaintiff's and the Plaintiff Class Members' patient communications with their medical providers as alleged herein contemporaneous with their making.

147. The intercepted communications include:

a. the content of patient registrations for various patient portals, including clicks on buttons to "Register" or "Signup" for said portals;

b. the content patient log-in and logout of the various patient portals, including clicks to "Sign-in," "Log-in," "Sign-out," or "Log-out."

c. the contents of communications that patients exchange inside various patient portals immediately before logging out of those portals; and

d. the contents of communications relating to appointments with medical providers.

148. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The cookies Facebook used to track patients' communications;

b. The patients' browsers;

c. The patients' computing devices;

d. Facebook's web-servers;

e. The web-servers of the Defendant Medical Providers' web properties where the Facebook Pixel was present; and

f. The Facebook Pixel source code deployed by Defendant to effectuate the sending and acquisition of patient communications.

149. Facebook is not a party to patient communications with their medical providers.

150. The Defendant Medical Providers sent to Facebook, and Facebook received, the content of patient communications through the surreptitious redirection of them from the patients' computing devices to Facebook.

151. Patients did not consent to the Defendant Medical Providers sending, or to Facebook's acquisition of, their patient portal, appointment, and phone call communications with their Defendant Medical Providers.

152. Neither Facebook nor the Defendant Medical Providers obtained legal authorization to obtain or convey patient communications with their medical providers relating to patient portals, appointments, and phone calls.

153. Facebook did not require any Defendant Medical Providers to obtain, and the Defendant Medical Providers did not obtain, the lawful rights to share the content of patient communications relating to patient portals, appointments, and phone calls.

154. Any purported consent that Facebook received from Defendant Medical Providers to obtain patient communications content was not valid.

155. In sending and in acquiring the content of patient communications relating to patient portals, appointments, and phone calls, Defendant had a purpose that was tortious, criminal, and designed to violate federal and state legal and constitutional provisions including:

a. A knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person;

b. A violation of 42 U.S.C. § 1320d-6, which is a criminal offensive punishable by fine or imprisonment;

c. Violation of state unfair business practice statutes;

d. Violation of HIPAA; and

e. Violation of Article I, section 1 of the California Constitution.

156. Defendant knew that such conduct would be highly offensive, as evidenced by Facebook's announcement in April 2018, that it would no longer allow advertising targeted based on health yet continued to use the Facebook Pixel on Defendant Medical Providers' properties for that purpose.

FOURTH CAUSE OF ACTION
NEGLIGENT MISREPRESENTATION
(Against Defendant and the Defendant Medical Providers Class)

157. Plaintiff hereby incorporate all other paragraphs as if fully stated herein.

158. Facebook represented to Plaintiff and the Plaintiff Class Members that a fact was true, namely, that before receiving the confidential information at issue, Facebook "requires" businesses "to have lawful rights to collect, use, and share [Plaintiff's and Plaintiff Class Members'] data before providing any data" to Facebook.

159. Defendant and Defendant Medical Providers represented to Plaintiff and Plaintiff Class Members Class that a fact was true, namely that they would not disclose the confidential information at issue for any reason or use not specifically listed in their Privacy Policies without obtaining Plaintiff's and Plaintiff Class Members' consents, and that they were compliant with policies related to sharing patient data and confidential information implemented or announced by third parties like Facebook.

160. Defendant's representations were not true.

161. Although Defendant may have honestly believed that its representations were true, Defendant had no reasonable grounds for believing its representations were true when they were made.

162. Defendant and the Defendant Class intended that Plaintiff and Plaintiff Class Members rely on their representations.

163. Plaintiff and Plaintiff Class Members reasonably relied on Defendant's representations.

164. Plaintiff and Plaintiff Class Members were harmed as set forth above.

165. Plaintiff and Plaintiff Class Members' reliance on Defendant's representations was a substantial factor in causing the harm.

EIGHTH CAUSE OF ACTION
NEGLIGENCE and NEGLIGENCE per se
(Against Defendant and the Defendant Medical Providers Class)

166. Plaintiff incorporates all previous paragraphs as if fully set forth below.

167. Plaintiff and Plaintiff Class Members entrusted their protected health information to Defendant Medical Providers, who owed them a duty to exercise reasonable

care in handling and using the PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from being conveyed to Facebook, and to promptly detect that it was being conveyed to Facebook without Plaintiff's and the Plaintiff Class Members' consent.

168. It was foreseeable to Defendant Medical Providers that incorporation of the Facebook Pixel onto their patient portals and web properties would result in the compromise of Plaintiff's and the Plaintiff Class's protected health information by conveying it to Facebook. By installing the Facebook Pixel onto their patient portals and web properties, the members of the Defendant Class acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Plaintiff's Class Members' PHI.

169. In addition, Defendant and Defendant Class Members had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

170. Defendant and the Defendant Class Members also had a duty to notify Plaintiff and the Plaintiff Class Members within a reasonable timeframe of any breach to the security of their PHI. This duty is required and necessary for Plaintiff and Plaintiff Class Members to take appropriate measures to protect their PHI, to be vigilant in the fact of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Defendant Class's conveyance of their PHI to Facebook.

171. Defendant and the Defendant Class owed these duties to Plaintiff and Plaintiff Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom the Defendant Class knew or should have known would suffer injury-in-fact from the Defendant Medical Providers' conveyance of Plaintiff's PHI to Facebook via the Facebook Pixel. The Defendant Class actively sought and obtained Plaintiff's and the Plaintiff Class's PHI via their patient portals and other web properties.

172. The risk that Facebook would try to gain access to the PHI and misuse it was foreseeable. Given that the Defendant Class holds vast amounts of PHI, and Facebook has sought access to that PHI and used it for advertising purposes in the past, as it has admitted, the Defendant Class was on notice of the need to protect Plaintiff's and the Plaintiff Class's PHI from Facebook.

173. PHI is highly valuable, and Defendant and the Defendant Class knew or should have known the risks in obtaining, using, handling, and storing, the PHI of Plaintiff and Plaintiff Class Members, and the importance in exercising reasonable care in handling it.

174. Defendant and the Defendant Class breached their duties by filing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in their handling and securing of the PHI of Plaintiff and Plaintiff Class Members, and in conveying that PHI to Facebook via the Facebook Pixel, which actually and proximately caused injuries to the Plaintiff and the Plaintiff Class.

175. Defendant and the Defendant Class also breached their duties by failing to provide reasonably timely notice to the Plaintiff and the Plaintiff Class Members of their

conveyance of their PHI to Facebook, which actually and proximately caused injuries to the Plaintiff and the Plaintiff Class.

176. As a direct and traceable result of Defendant's negligence or negligent supervision, Plaintiff and Plaintiff Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

177. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's actual, tangible, injury-in-fact and damages, including, without limitation, the improper disclosure of PHI, lost benefit of their bargain, lost value of her PII, and lost time and money incurred to mitigate this improper disclosure that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which she continues to face. The Defendant Class's breach similarly caused damages to the Plaintiff Class.

178. Defendant's statutory violations of the FTC Act, HIPAA, the ECPA and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

179. But for Defendant and the Defendant Class's wrongful and negligent breach of their duties owed to Plaintiff and Plaintiff Class Members, Plaintiff and Plaintiff Class Members would not have been injured. These injuries were the reasonably foreseeable result of Defendant and the Defendant Class's breach of their duties. Defendant and the Defendant Class knew or should have know that they were failing to meet their duties and

that their breach would cause Plaintiff and Plaintiff Class Members to suffer the foreseeable harm associated with the exposure of their PHI.

180. Had Plaintiff and Plaintiff Class Members known that Defendant and the Defendant Class would not adequately protect their PHI, Plaintiff and Plaintiff Class Members would not have entrusted Defendant with their PHI.

181. As a direct and proximate result of Defendant and the Defendant Class's negligence *per se,* Plaintiff and Plaintiff Class Members have suffered harm, including:

a. General damages for invasion of their privacy rights in an amount to be determined by a jury without reference to specific pecuniary harm;

b. Sensitive and confidential information including patient status and appointments that Plaintiff and Plaintiff Class Members intended to remain private are no longer private;

c. Defendant eroded the essential confidential nature of the patient-provider relationship;

d. Defendant took something of value from Plaintiff and Plaintiff Class Members and derived benefits therefrom without Plaintiff's and Plaintiff Class Members' knowledge or informed consent and without sharing the benefit of such value;

e. and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court:

1. Certify the proposed Plaintiff Class, designating Plaintiff Afrika Williams as the named representative of the Class, and designating the undersigned as Class Counsel;

2. Certify the proposed Defendant Medical Provider Class, designating Defendant DukeHealth as the named representative of the Defendant Class, and designating its counsel as Defendant Class Counsel;

3. Award compensatory damages, including statutory damages where available and nominal damages, to Plaintiff and the Plaintiff Class against Defendant and the Defendant Class for all damages sustained as a result of Defendant's and the Defendant Class's wrongdoing, in an amount to be proven at trial, including interest thereon;

4. Award punitive damages on the causes of action that allow for them and in an amount that will deter Defendant, the Defendant Class, and others from like conduct;

5. Award attorneys' fees and costs, as allowed by law;

6. Award pre-judgment and post-judgment interest, as provided by law; and,

7. For such other, further, and different relief as the Court deems proper under the circumstances.

DATED: July 28, 2023

By: */s/James Harrell*

Peter H. Burke*
James Harrell, NC Bar No. 47787
CRUMLEY ROBERTS, LLP
2400 Freeman Mill Road, Suite 200
Greensboro, NC 27406
Telephone: (366) 333-9899
phburke@crumleyroberts.com
jrharrell@crlegalteam.com

Karen Hanson Riebel*
Kate M. Baxter-Kauf*
Maureen Kane Berg*
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com
mkberg@locklaw.com

** Special Appearances Entered*
Attorneys for Plaintiff and Proposed Class Counsel

CERTIFICATE OF SERVICE

I hereby certify that on this 28th of July, 2023, I electronically filed the foregoing **Amended Complaint – Class Action** with the Court using the CM/ECF System, which will automatically serve all attorneys of record via the Courts CM/ECF System.

/s/James R. Harrell
James R. Harrell
Attorney for Plaintiff